As practices work hard to be recognized for their great patient care and improved satisfaction, they are faced with a new challenge: medical identity theft. Most practices are aware of identity theft, which is the stealing of another person’s identity; now they must prevent it from happening in their own practice.

**Definition**

Medical identity theft occurs when a person is able to gain access to someone else’s health insurance or medical information and then uses that information to obtain medical treatment. An insurance company may unknowingly make payment on the claim believing that it is the correct patient who is being treated.

Needless to say, medical identity theft is illegal and unethical. It jeopardizes the entire medical system and how it should be helping patients. Just as identity theft can be costly to the victim, medical identity theft is costly to the patient, the practice, and the insurance company. Insurance companies would be paying for claims for patients who are not insured by that company.

In addition, insurance companies track diagnoses and treatments of patients. When someone other than the patient uses the insurance and has a procedure performed, the insurance company is aware of this. Later, if the “real” patient comes in with similar symptoms or the same disease, the insurance company would question the diagnosis and any potential treatment, and possibly deny coverage for the treatment the patient needs. An example of this would be an identity thief who uses someone else’s insurance information to pay for having his gallbladder removed. Later, the real person comes in with symptoms of gallbladder disease. The insurance company would not approve having the surgery done a second time, because that would be impossible. Fraud is detected after a serious problem has been created.

**Medical Identity Theft Is Costly**

Medical identity theft is not only costly, but it also could potentially have fatal results. When patients’ medical records include misinformation, the provider treating the patient is misguided by the incorrect data, and therefore may not offer the best treatment options. This becomes not only a financial matter but also a quality-of-care issue.

How easy is it for a person to commit medical identity theft? Actually, it is easier than one might think. The thief needs your name, date of birth, possibly your Social Security number, and your insurance card (or, if not the actual card, the details off of the card, including the member name, group number, and identification number). If the thief has access to a way of making a copy of the card, it would be easy for a practice to use the copy and assume it is correct information.

Therefore, a practice should institute policies and procedures to prevent medical identity theft. This includes preventing outsiders from gaining access to the information within the office, as well as not accepting patients who are using a false identity. At the very least, a practice should require photo identification from patients. Train your employees to understand the dangers of medical identity theft and how they can take action to prevent it in your practice. Gathering benefit and eligibility information prior to a patient’s visit also

---


**Is Your Practice at Risk for Medical Identity Theft?**

Are you taking the proper steps to prevent this crime?

BY DONNA WEINSTOCK

Medical identity theft is not only costly, but could potentially have fatal results.
To protect your practice from seeing medical identity theft in your office, it should also state the procedures to follow should the practice suspect an identity breach. Protecting patients’ privacy should be included in your manual. Include any incident report forms that are part of your practice. Staff members need ongoing training to understand the procedures to be followed. Insurance cards, credit card information, and patient information sheets must be locked to prevent unauthorized persons gaining access to the information. This is the type of information that hackers and thieves look for. It takes very little to steal an identity and not much more to steal a medical identity. Leaving credit card information in a folder on a desk is an invitation for a thief to use it for unauthorized purposes.

To protect your practice from seeing patients using a stolen identity, it is important to ask for photo identification from the patient. Most often, a driver’s license is sufficient. Patients who are using their insurance should bring their insurance card. Allowing copies offers potential risks; therefore, the original should be required. Matching addresses and information between the photo identification and other data collected will deter unauthorized usage.

Medical identity theft can be deliberate, as when the patient shares his or her insurance card or other personal information with someone he or she knows, or it could happen unknowingly when an insurance card is stolen. Helping your patients stay safe from medical identity theft should be part of your practice’s policies:

- Make patients aware of medical identity theft and the potential dangers it may cause to their medical record and finances. They need to understand that this is dangerous to them as well as illegal.
- Suggest patients keep their insurance card in a secure place, not carrying it with them unless they have a physician appointment or pending procedure.
- Make sure patients know that they should never share their insurance healthcare card with anyone. No one else should use their insurance when seeing a physician or going to any healthcare appointment. It is illegal and dangerous to use someone else’s healthcare insurance.
- Instruct patients to monitor any explanation of benefits (EOB) they receive. EOB forms show the services that patients receive. If a patient receives an EOB for a service he or she did not have, the patient should contact the insurance company, the physician, and possibly the authorities by filing a police report.
- Patients should know that they should not share medical information with unknown persons, just as they should not reveal any personal information to just anyone who asks for it (via telephone or otherwise).
- Patients should be allowed to review or request copies of their medical records for accuracy.
- Patients should track their credit through credit reports. If a patient finds that he or she owes a health-

Medical identity theft can happen inside a practice. Fraudulent billing of claims for patients who did not undergo a particular procedure in an attempt to add revenue to the practice is illegal. Monitoring by the practice is essential to ensure that all billing is accurate.

It is important to protect your practice from possible inaccurate or illegal information. This can be done in several ways:

- Hire employees who are honest and understand the dangers and risks of medical identity fraud in your practice. Do reference and background checks on all new hires.
- Initiate access limits so that employees have access only to data they need to perform their specific job. Clinical personnel most likely will not need access to the billing portion of your electronic health record. A billing employee may need only limited access to clinical information. Insurance companies often request operative reports, office notes, and other supporting documentation that billers may need to access. Front desk receptionists primarily need access to the demographics. Restrict data according to a “need to know” basis.
- Control which employees have access to the administrative portion of your computer system. This may include the server as well as the “sys-

Helping your patients stay safe from medical identity theft should be part of your practice’s policies.
Theft (from page 124)

The fewer staff members that access the administrative portion, the safer and more secure the system is.

- Keep a scanner at the front desk and scan driver’s licenses, insurance cards, and other pertinent information into your electronic health record. For those practices without an electronic health record (EHR) system, a copy of the patient’s identification should be placed in his or her chart.
- Train staff to look for forged or inaccurate information. This may include a picture ID that does not resemble the patient or data that don’t match what is already in the healthcare record. All departments should be looking for inaccuracies that indicate potential data breaches. Your billing department may see charges that don’t fit with other visits, or other potential discrepancies.
- Track anything suspicious until you are sure that a fraud has occurred. Then follow your procedure to handle the theft.

Your policies and procedures for handling medical identity theft should include speaking with the patient to determine if a breach has occurred or if, in fact, it was an error. If you suspect a breach, the patient must be notified, as must the authorities.

Your procedure manual should include a procedure to ultimately separate the records to correct the medical identity breach. The thief’s medical record should be taken out of the patient’s record and placed in its own chart. This separation of charts would need to be documented. If it is impossible to separate out the thief’s data, there should be documentation that the medical record contains inaccurate information, and a list of what portions are inaccurate.

The documentation process forms to be used and other procedures to be followed must be clearly stated and detailed. You must clearly state the consequences to an employee who participates in medical identity theft either by knowingly allowing it to happen or by billing fraudulent charges to insurance carriers.

Reducing risk to prevent identity theft is the goal. Many EHR systems have built-in programs that can help detect inaccuracies in a medical record chart. By contacting your EHR company, you can determine if there are safeguards that your practice should take.

Under the Affordable Care Act (ACA), it is likely that the risk of medical identity theft should decline. With the ACA mandating the institution of EHRs, practices are better able to streamline their processes and improve the quality of care and accuracy of the medical records. The threat of fraudulent use of medical data should lessen. When the data are stored on a secure server, it is more difficult to gain access.

Offering healthcare coverage to more individuals lessens the likelihood or need for identity theft, because fewer patients are without health insurance. However, higher deductibles will mean greater out-of-pocket expenses for patients, which may lead to temptation to commit medical identity theft.

Conclusion
Medical identity theft is becoming more prevalent as thieves and hackers become more creative in stealing medical identities. Practices need to take action to ensure that the patients they are seeing are the same ones whose insurance they are billing. Practices also need to keep patient and medical information safe and secure so patients know they are protected. Following state and federal guidelines, and having procedures in place and systems to monitor that the procedures are being followed, will protect the practice and patients from unauthorized use of medical data.

Suggested Reading

Donna Weinstock is president, Office Management Solution, Northbrook, Illinois; e-mail: donna@officemanagementsolution.com.